

JOSEPH W. PRICE
ALBIN H. GESS
FRANKLIN D. UBELL
MICHAEL J. MOFFATT
GORDON E. GRAY III
BRADLEY D. BLANCHE

RICE, GESS & UBELL
ATTORNEYS AT LAW

2100 S.E. MAIN STREET, SUITE 250

IRVINE, CALIFORNIA 92614-6238

A PROFESSIONAL CORPORATION
TELEPHONE: (949) 261-8433
FACSIMILE: (949) 261-9072
FACSIMILE: (949) 261-1726

e-mail: pgu@pgulaw.com

DRAWINGS - FOURTEEN (14) SHEETS

Applicant(s):

Makoto Tatebayashi et al.

Title:

ENCRYPTION METHOD, ENCRYPTION
APPARATUS, DECRYPTION METHOD, AND
DECRYPTION APPARATUS

Attorney's
Docket No.:

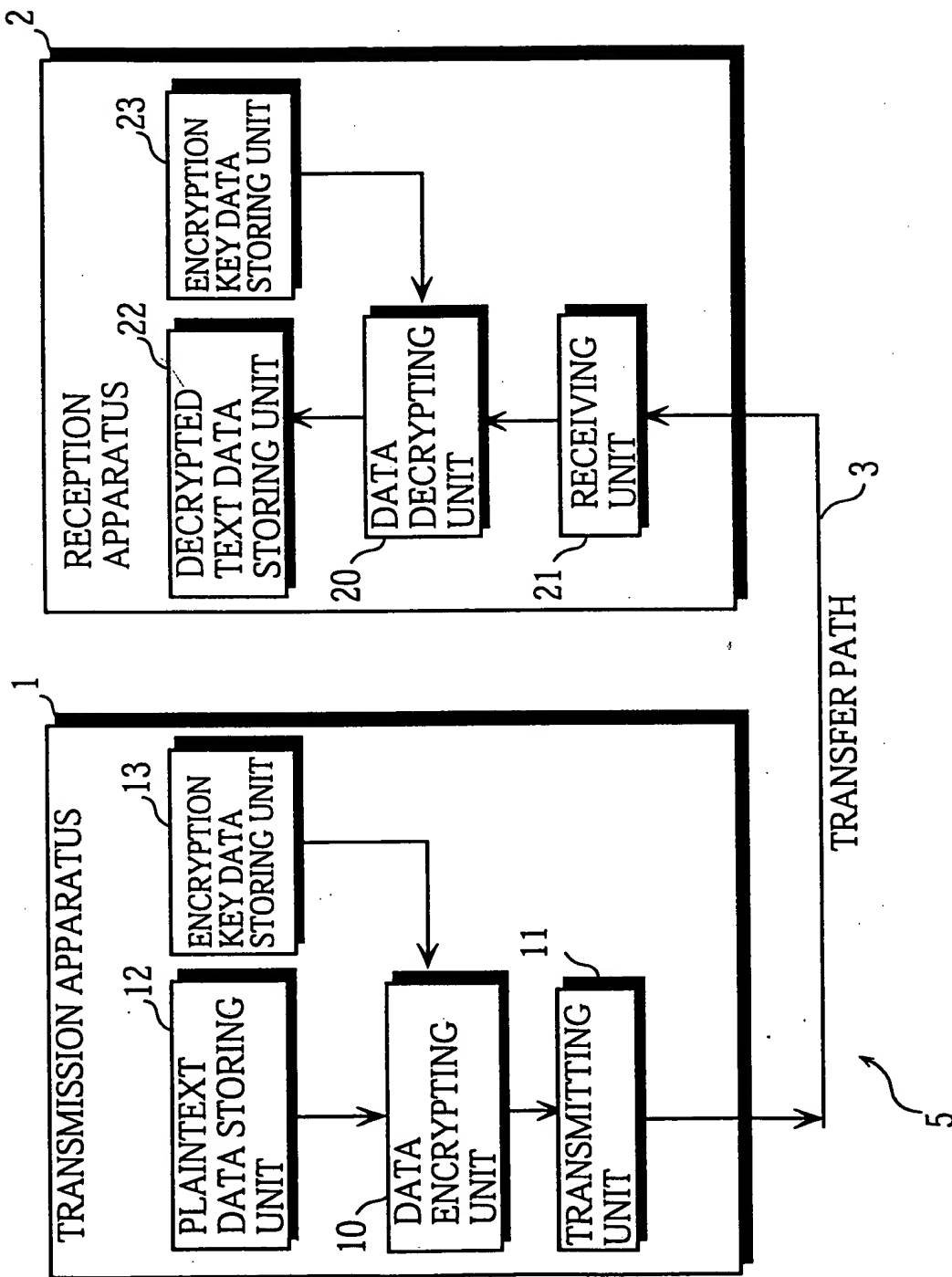
NAK1-BM08

"EXPRESS MAIL" MAILING
LABEL NO. EL230379070US

DATE OF DEPOSIT: August 15, 2000

09638616-081500

FIG.1



5
ENCRYPTED COMMUNICATION SYSTEM

FIG.2

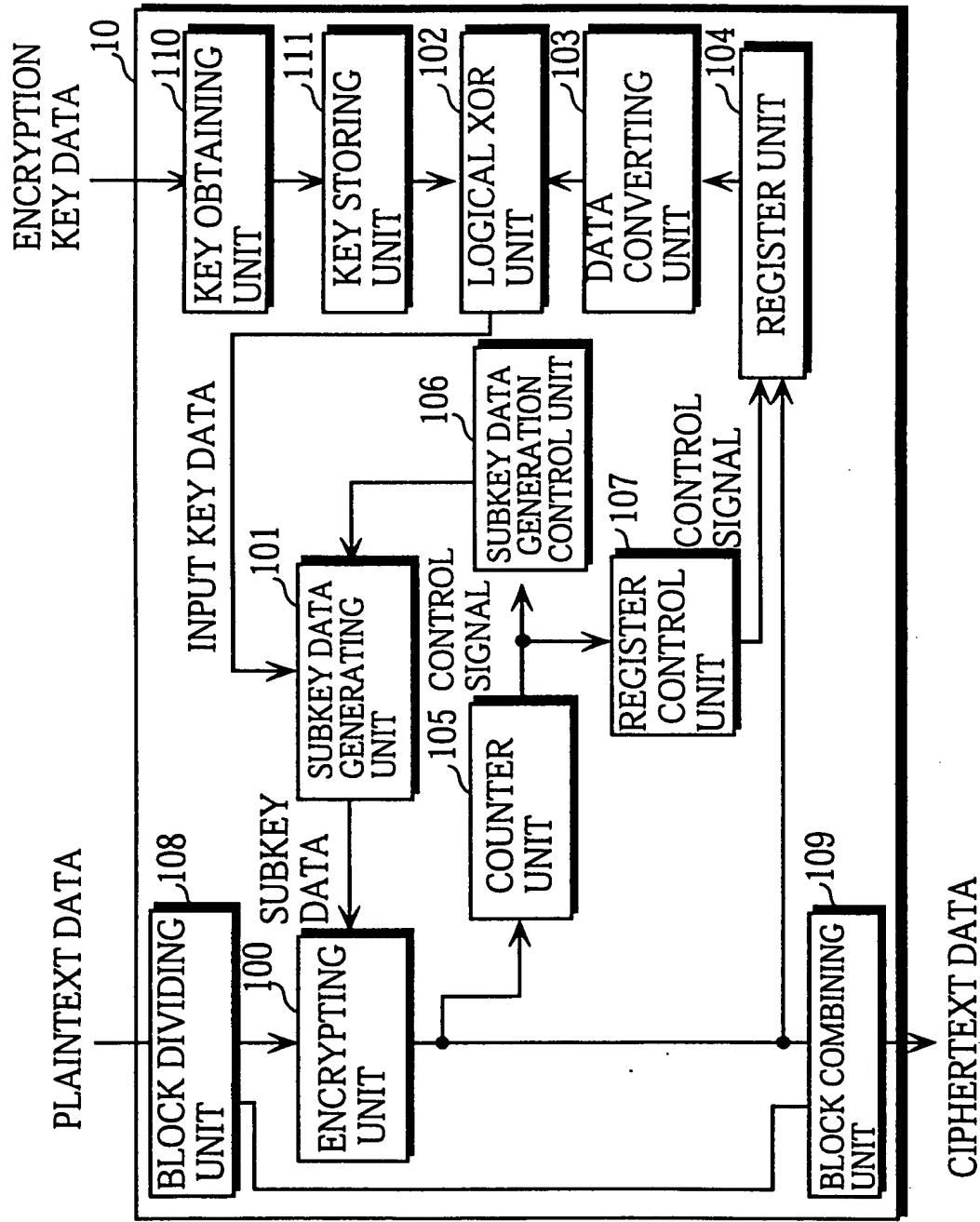


FIG.3

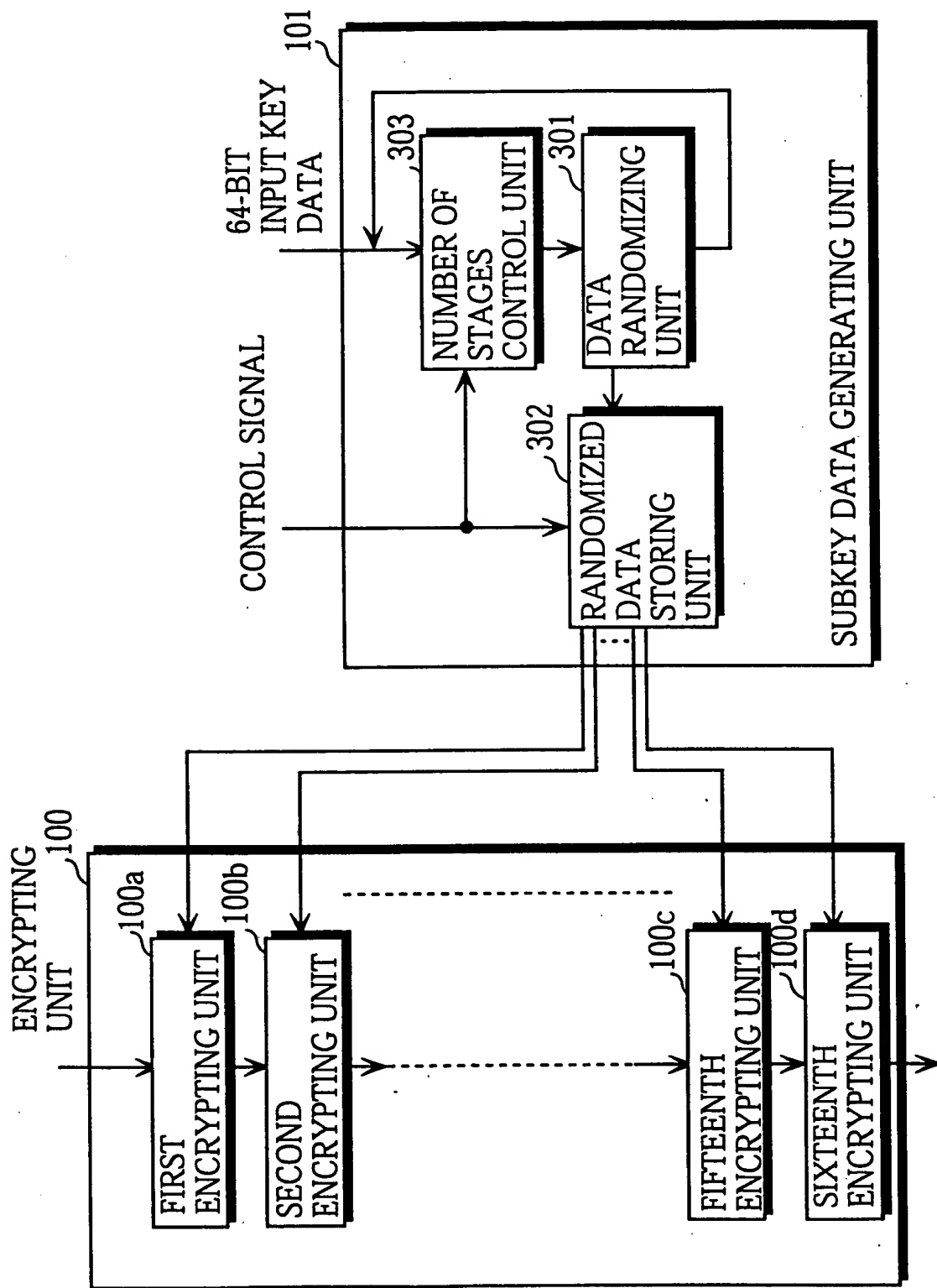


FIG. 4

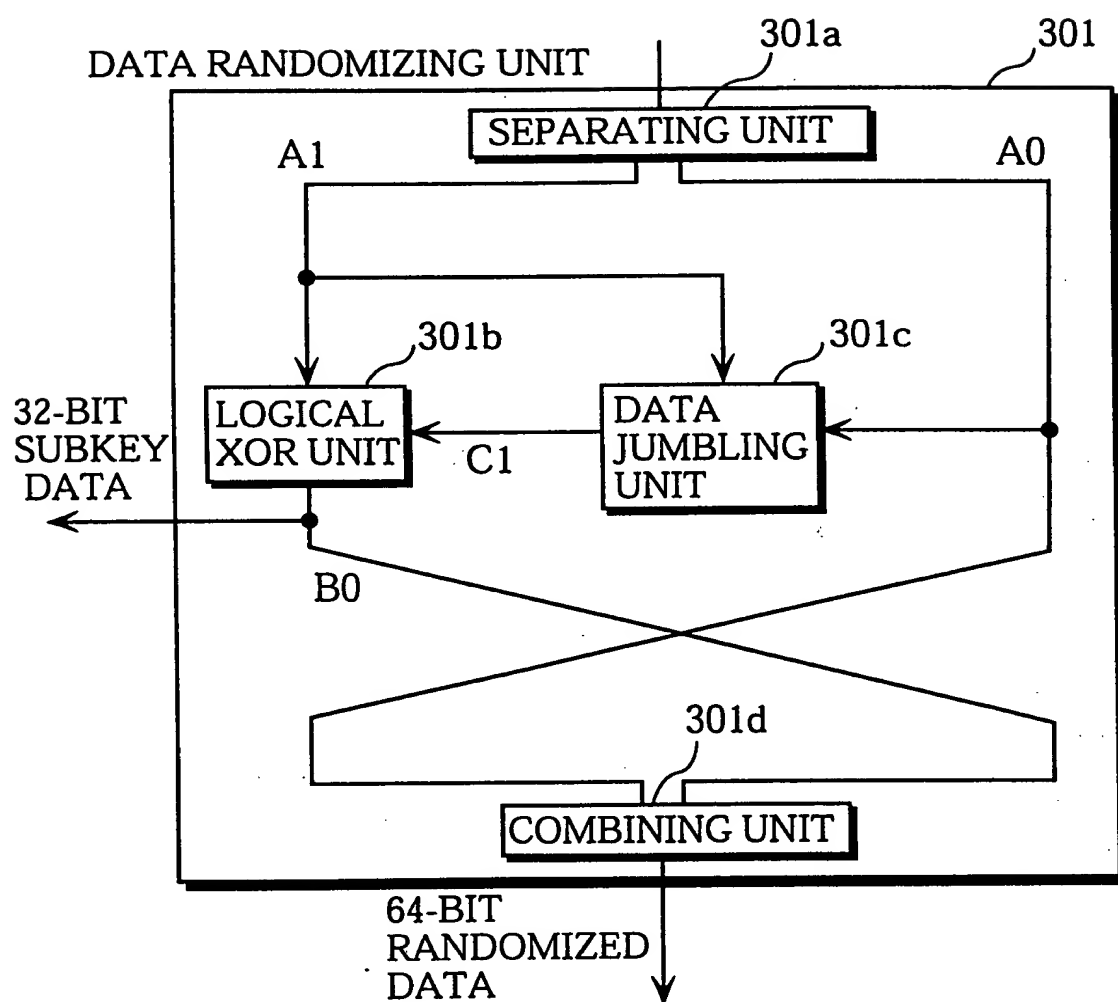


FIG. 5A

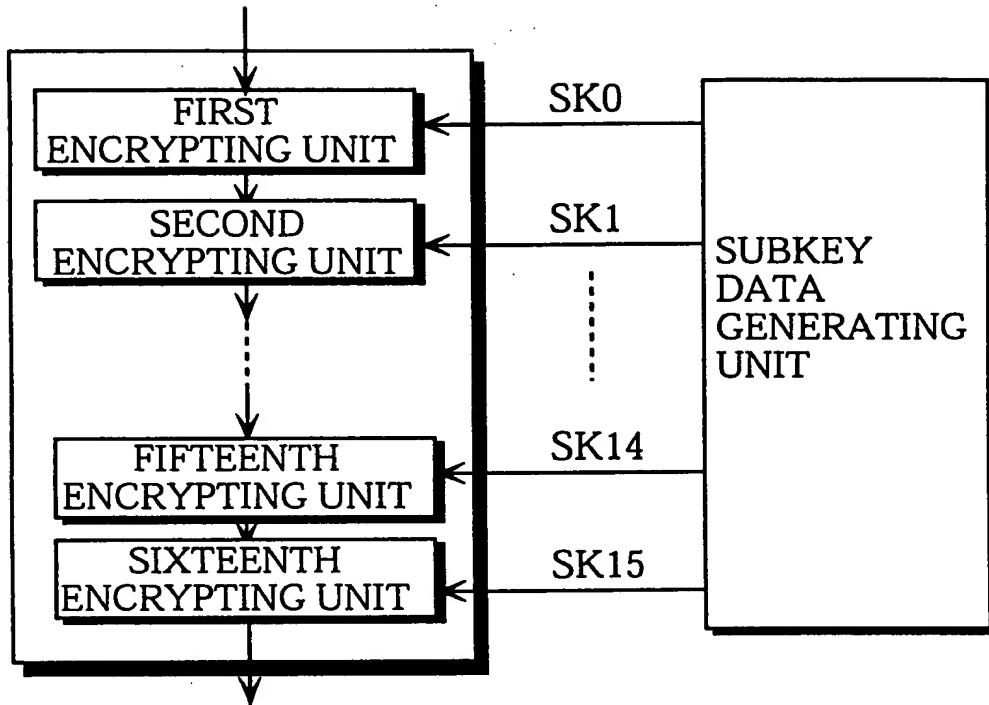
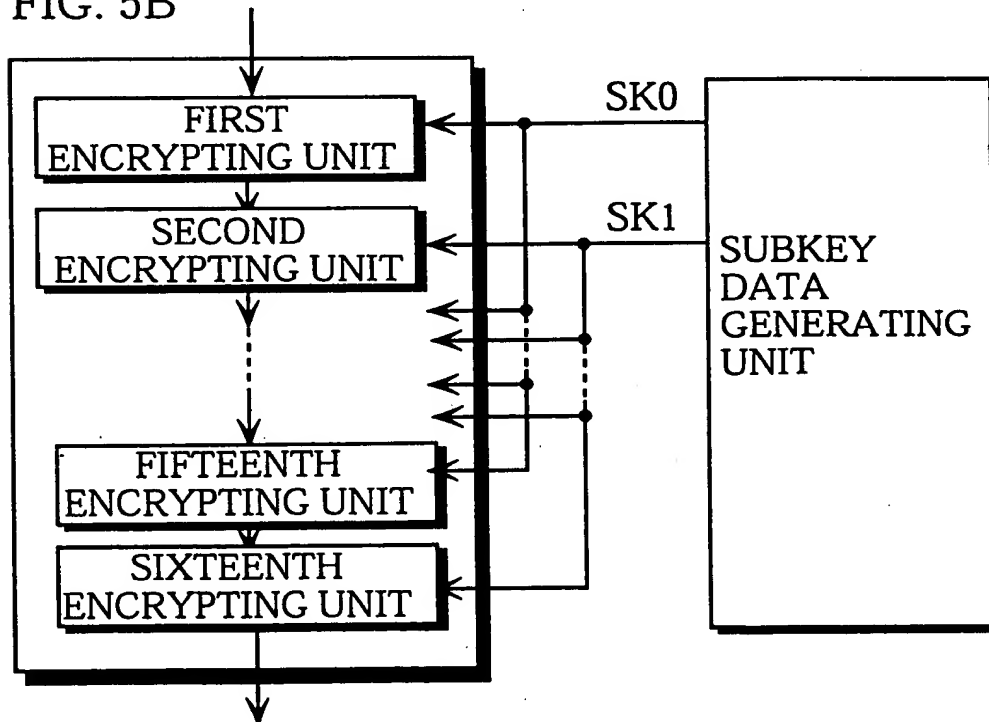


FIG. 5B



09638616-001500

FIG.6

COUNT VALUE	INPUT KEY DATA	SUBKEY DATA GENERATION TYPE
0	$EK(+) f(IV)$	A
1	$EK(+) f(C_0)$	B
2	$EK(+) f(C_1)$	B
\vdots	\vdots	\vdots
$2^{10}-1$	$EK(+) f(C_{2^{10}-2})$	B
0	$EK(+) f(IV)$	A
1	$EK(+) f(C_0)$	B
2	$EK(+) f(C_1)$	B
\vdots	\vdots	\vdots
$2^{10}-1$	$EK(+) f(C_{2^{10}-2})$	B
0	$EK(+) f(IV)$	A
\vdots	\vdots	\vdots

FIG. 7

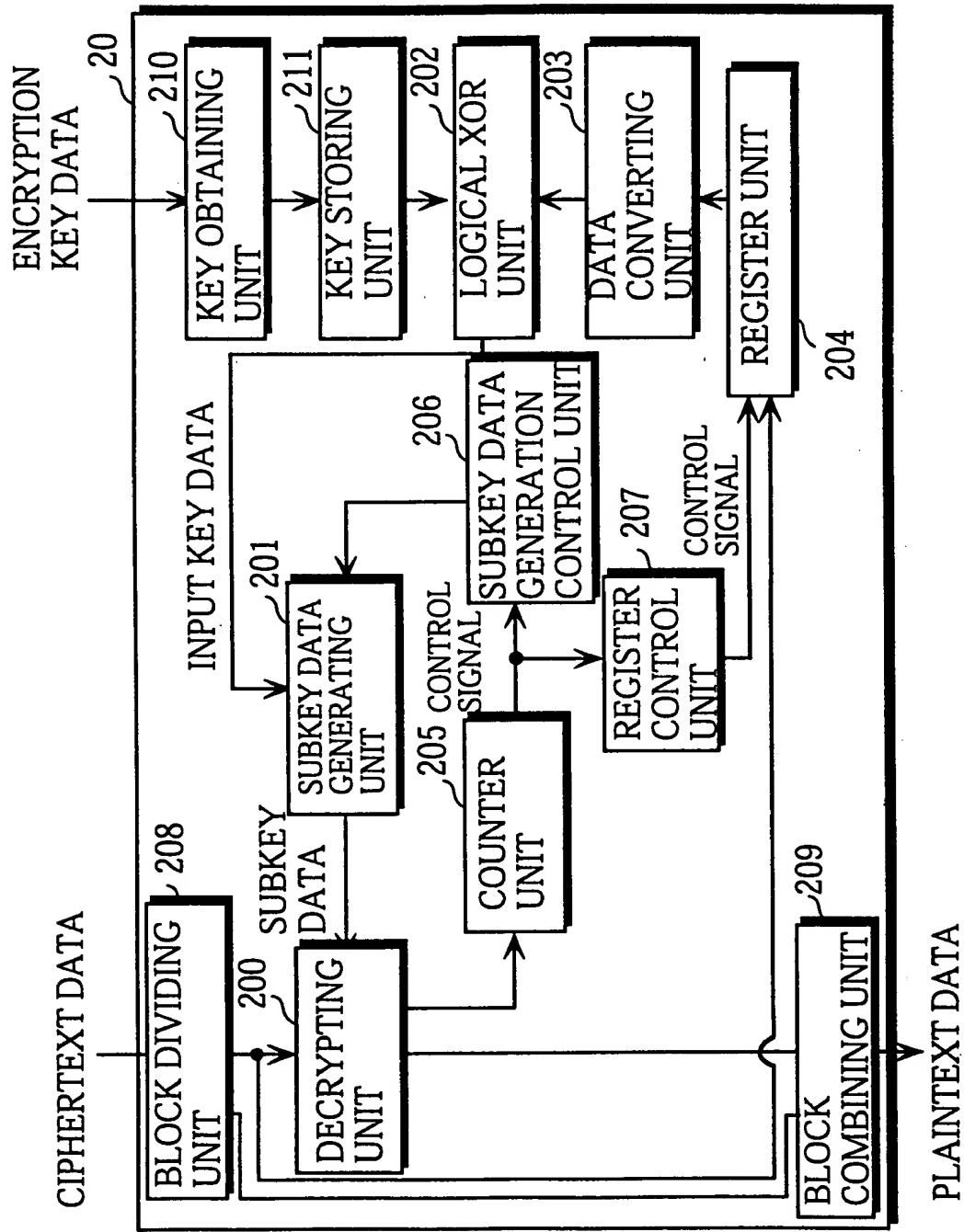


FIG. 8

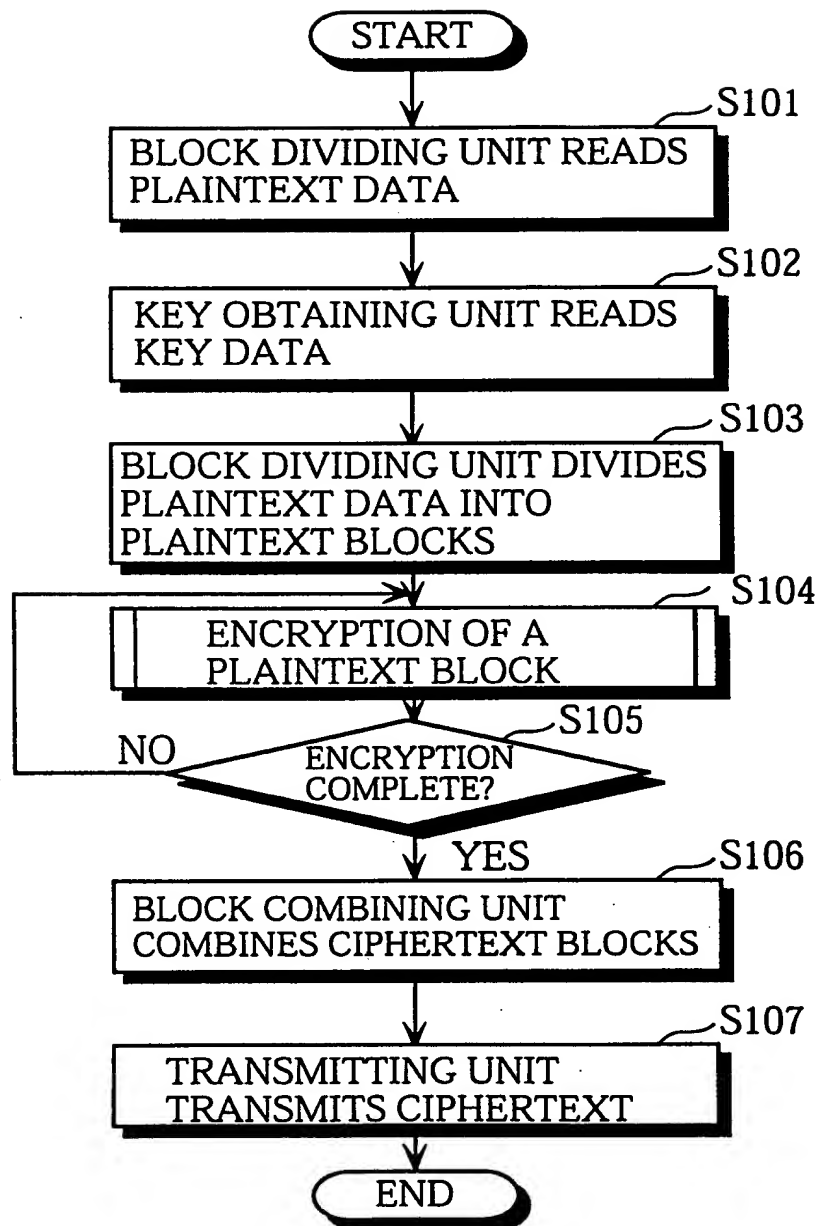


FIG. 9

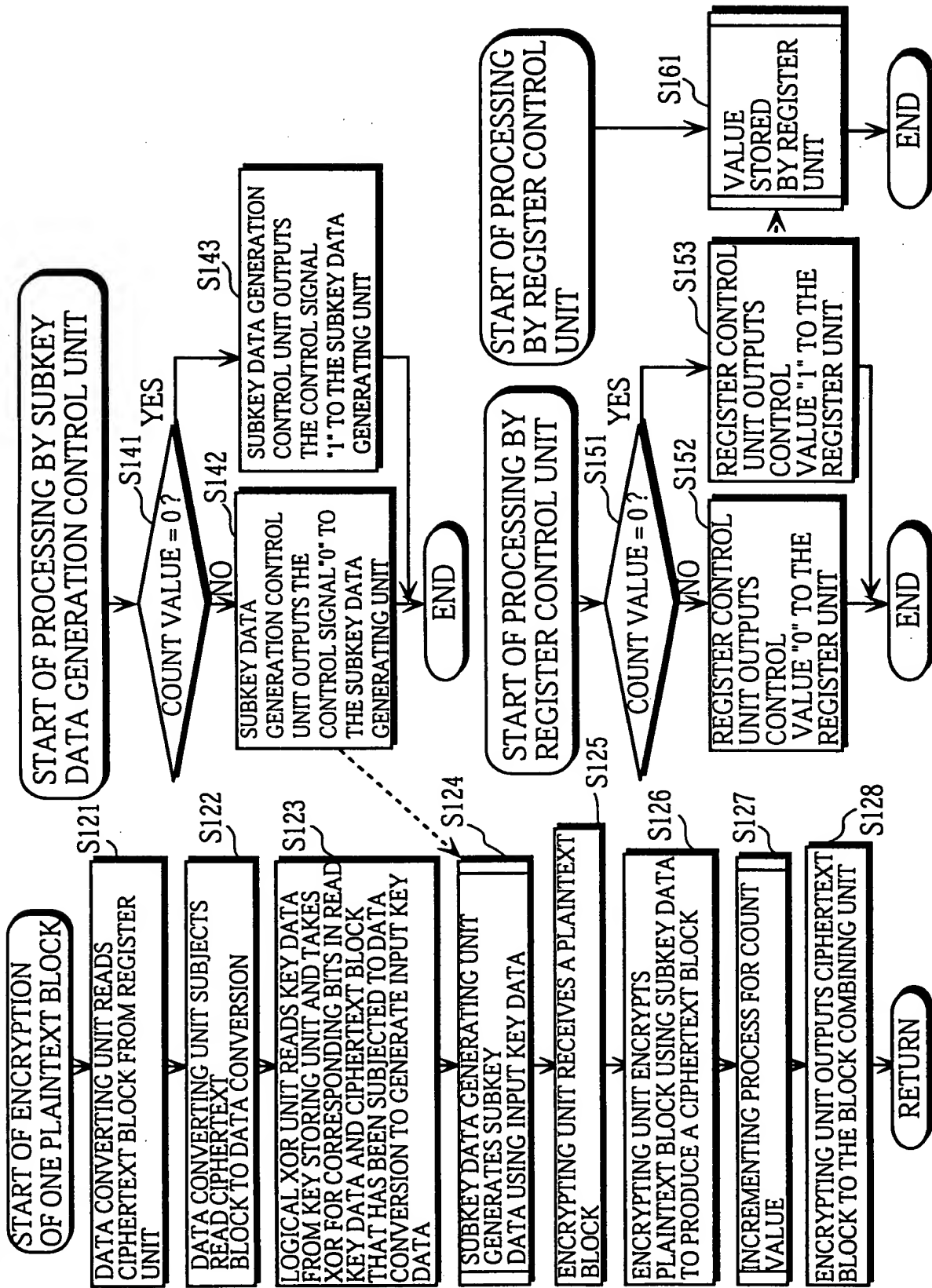


FIG. 10

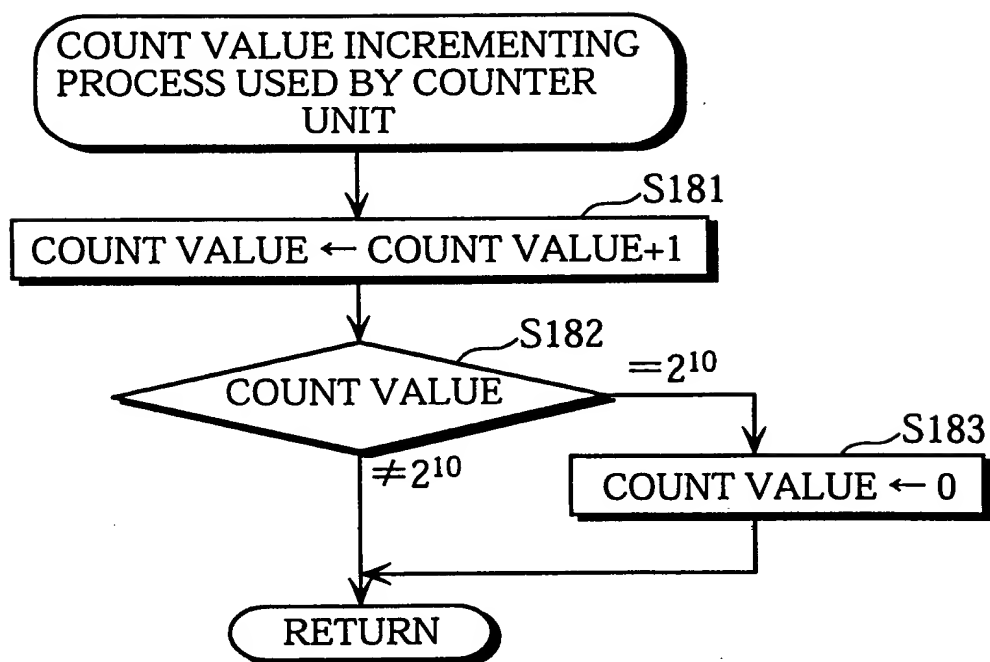


FIG. 11

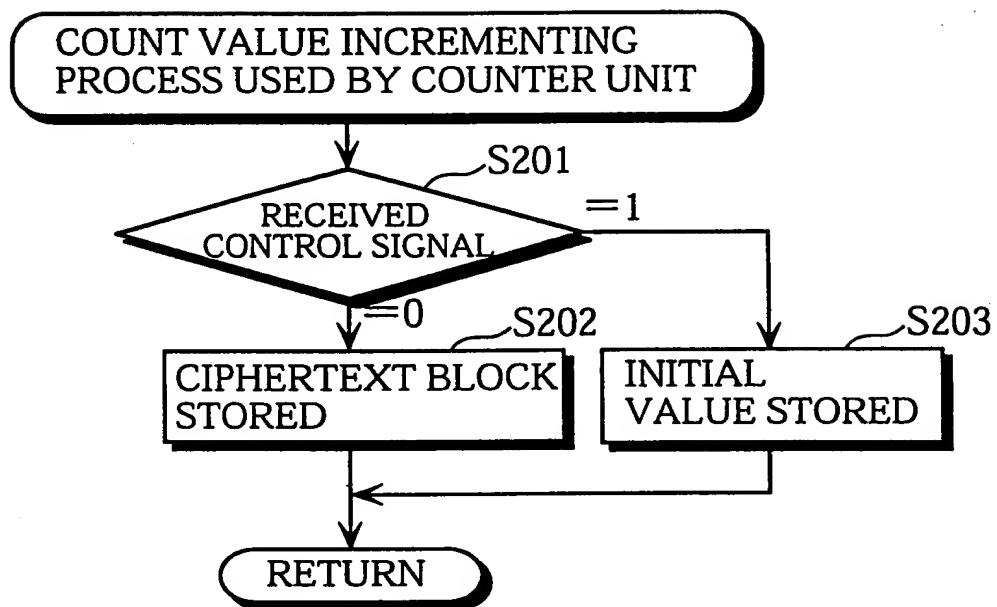
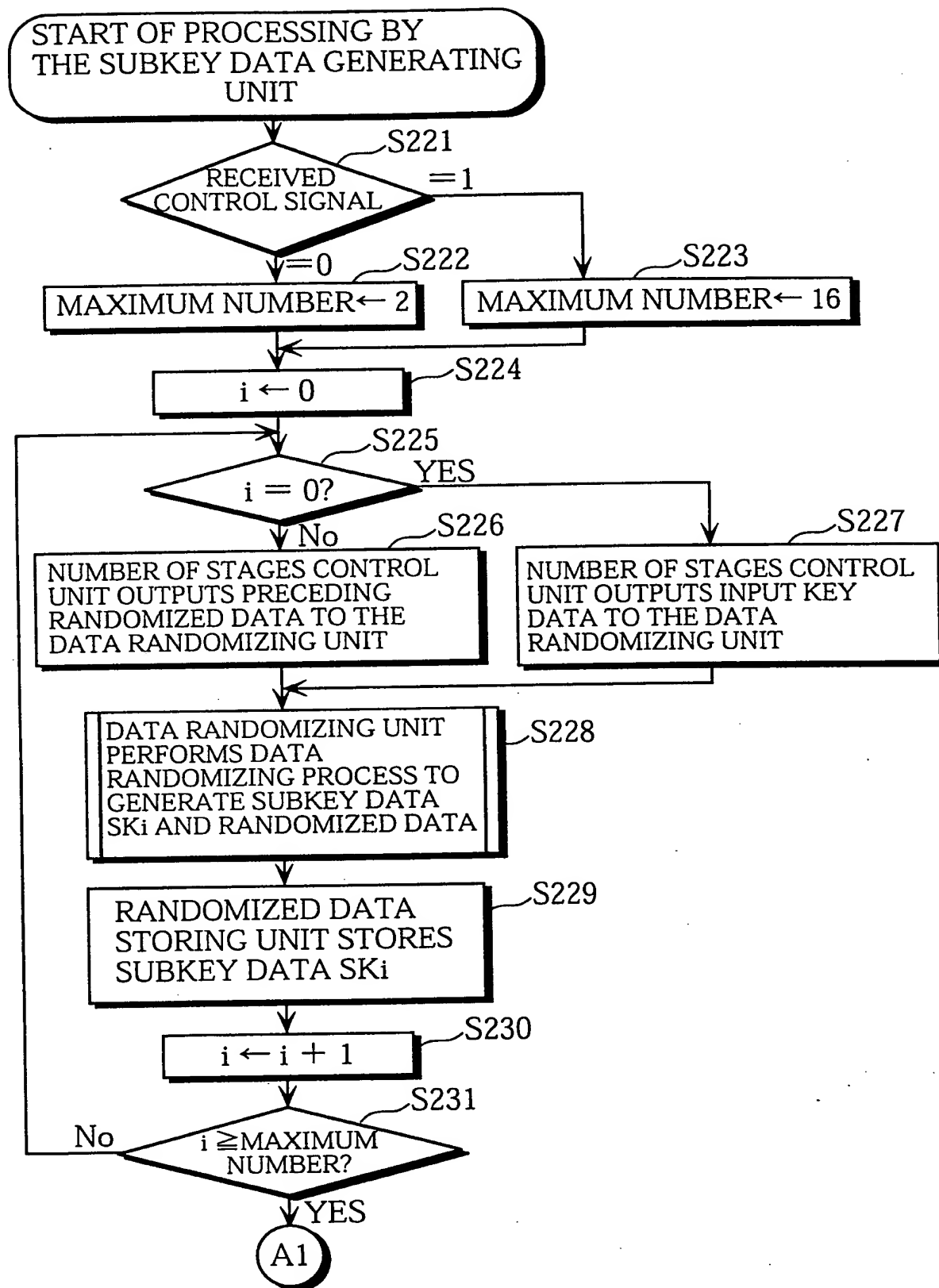


FIG. 12



005180" 9158E360

005780" 9T982960

FIG. 13

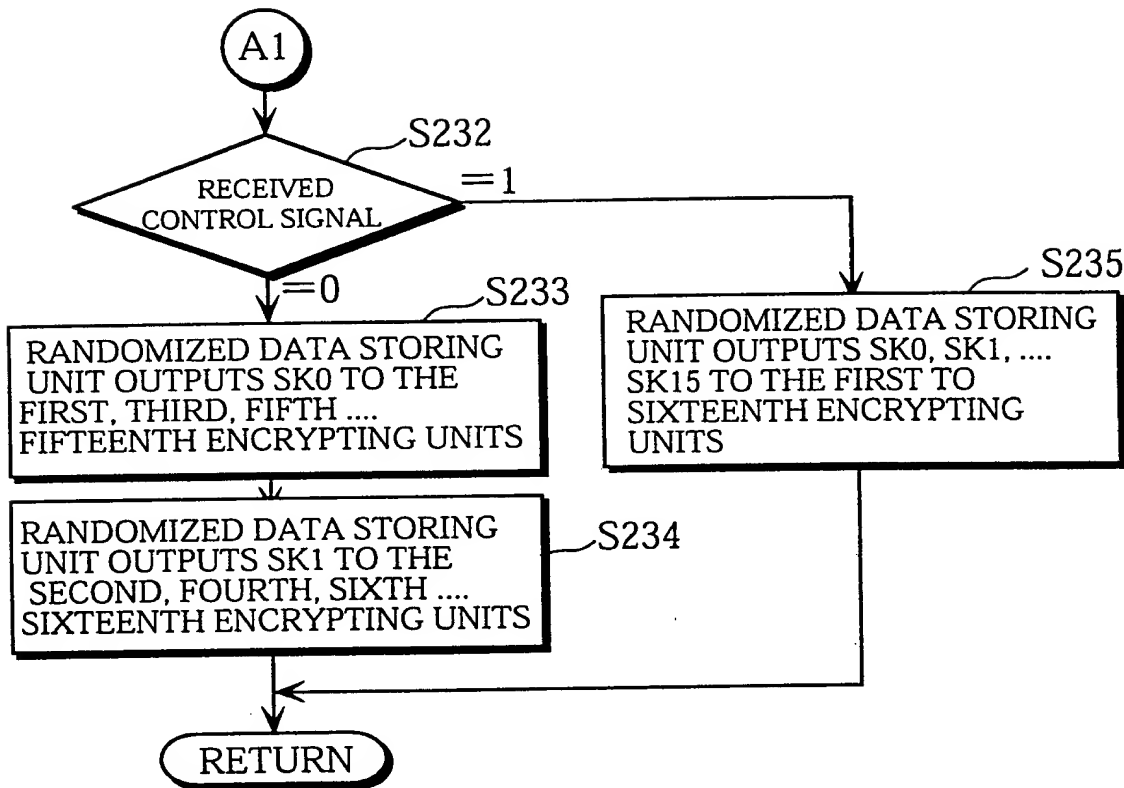


FIG.14

